SC-ISAC ADVISORY ***SC-ISAC ADVISORY 8*** **DATE(S) ISSUED: 8-23-2007**

S.C. INFORMATION SHARING AND ANALYSIS CENTER BULLETIN

SUBJECT: Multiple Web site Defacements

SCOPE: Organization Wide – Government and Private Sites

BULLETIN:

There has been a major increase in the amount of Web site defacement exploitations by hackers in Turkey. Several sites in South Carolina have been targeted as well as several very high profile sites affiliated with government.

Some of the groups claiming credit include: “iskorpitz,” “casus-team,” “Ay Yildiz Team,” “saldiriteam,” “teknopatron.” There are other groups being investigated at this time.

Attack vectors include: SQL Injection including MS-Access and other flat file databases accessible through MDAC; permission based exploits also appear to have been used, e.g. UID/Password guessing.

Agencies already participating in the CyberSentry program have upgraded intrusion detection systems configured to detect some of this activity. Review daily reports for information.

RECOMMENDATIONS:

- **Short-term prevention**
  - Perform an application risk assessment to determine and then fix application security vulnerabilities.
  - Install anti-virus software and keep its virus signature files up-to-date.
  - Block executable and unknown file types being uploaded to Web servers.
  - Route or proxy Web site traffic through virus and other types of filters.
  - Change passwords routinely and maintain a good password policy.

- **Long-term prevention**
  - Periodically, or whenever application changes occur, perform an application risk assessment to determine and then fix application security vulnerabilities.
  - Install only the minimum essential operating system configuration – use only those software packages containing files and directories that are needed to operate the computer.
  - Install patches to correct known deficiencies and vulnerabilities.
  - Install the most secure and up-to-date versions of system applications.
  - New updates or installations after initial installation was performed can restore undesired access privileges.

- Review all privilege and access requirements and then grant (add back in) privilege and access only as needed, following the principle "deny first, then allow."
- Enable as much system logging as possible to have access to detailed information (needed for in-depth analysis of an intrusion).
- Active content such as databases should only have necessary access privileges.
- Whenever possible protect and isolate Web servers and database servers on secure network segments.
- Always use encrypted access for remote administration or content updates.
- Monitor and inspect network activities.

REFERENCES:

Carnegie Mellon:
http://www.sei.cmu.edu/publications/documents/sims/sim010.html

CERT:
http://www.cert.org/
http://www.cert.org/certcc.html

SC-CSIRT:
https://secure.sc.gov
http://www.sc-isac.sc.gov/

Definition / Information:
Wikipedia: http://en.wikipedia.org/wiki/Defacement_%28vandalism%29

SC-ISAC CONTACT INFORMATION:

E-mail: SC-ISAC@cio.sc.gov

Telephone: **+1 803.896.1650 SC-ISAC**
+1 803.896.0001 (24-hour hotline)

Fax: **+1 803.896.0099**

Postal Address: **SC-ISAC**
CIO Budget and Control Board
4430 Broad River Road
Columbia S.C. 29210

SC-ISAC is available via hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday.

USING ENCRYPTION:

We strongly urge you to encrypt sensitive information sent by e-mail. Our public PGP key is available from: http://www.secure.sc.gov/site/sc-isac.txt.

NO WARRANTY

Any material furnished by SC-ISAC is furnished on an "as is" basis. SC-ISAC makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. SC-ISAC does not make any warranty of any kind with respect to freedom from patent, trademark or copyright infringement.